A nonabelian group with equally many endomorphisms and partial isomorphisms

A computer-assisted counterexample to Kourovka Problem 19.20

Kyrylo Muliarchyk

Abstract

We construct a nonabelian group G of order 512, nilpotency class two and exponent four, such that

$$|\operatorname{PIso}(G)| = |\operatorname{End}(G)| = 2\,164\,260\,864 = 129 \cdot 2^{24}.$$

This gives a negative answer to Problem 19.20 in the Kourovka Notebook. The group is specified by an explicit multiplication law. The endomorphism count has a direct algebraic proof. The partial-isomorphism count is proved by exhaustive finite quadratic-map enumeration, with exact isomorphism tests and automorphism orders. The complete printable certificate and standalone verification programs are included in this PDF. No group database is used in the verification, and no assertion of minimal order is made.

1 The problem and the result

Question. The following problem appears in the Kourovka Notebook [2, p. 135].

> **19.20.** For a finite group G, let $\operatorname{End}(G)$ denote the semigroup of endomorphisms of G, and $\operatorname{PIso}(G)$ the semigroup of partial isomorphisms of G (isomorphisms between subgroups of G). If G is abelian, then $|\operatorname{End}(G)| = |\operatorname{PIso}(G)|$. Is the converse true?
>
> *P. J. Cameron*

The trivial subgroup is included. Thus the unique isomorphism $1 \to 1$ and the trivial endomorphism are each counted once; no empty partial map is adjoined. Write $P(G) = |\operatorname{PIso}(G)|$ and $E(G) = |\operatorname{End}(G)|$. Cameron's equality for finite abelian groups is proved in [1].

Theorem 1.1. *The group G defined in Section 2 is nonabelian, has order 512, and satisfies*

$$|\operatorname{PIso}(G)| = |\operatorname{End}(G)| = 129 \cdot 2^{24}. \tag{1.1}$$

Moreover,

$$G' = \Phi(G) \cong C_2^3, \qquad Z(G) \cong C_2^4, \qquad |\operatorname{Aut}(G)| = 2^{24}.$$

Section 3 determines the endomorphisms directly from the quadratic square map. Section 4 proves the exhaustive counting method and applies it to the partial isomorphisms. Appendix A contains all type records, with representatives and automorphism orders; Section 5 explains how to regenerate them. Thus the full equality is established by a finite counting proof, without requiring a structural bijection between the two sets.

2 The group

All vector spaces in the construction are over $\mathbf{F}_2$. Put

$$V = \mathbf{F}_2^6, \qquad W = \mathbf{F}_2^3.$$

Write $v = (a, b, c, d, e, t)$ and $u = (a', b', c', d', e', t')$. Define the bilinear map $f : V \times V \to W$ by

$$\begin{aligned} f_1(v,u) &= aa' + dd' + ea' + db', \\ f_2(v,u) &= cc' + dd' + eb' + dc', \\ f_3(v,u) &= bb' + cc' + ec'. \end{aligned} \tag{2.1}$$

Define multiplication on $V \times W$ by

$$(v, w)(u, z) = (v + u,\ w + z + f(v, u)). \tag{2.2}$$

Bilinearity gives

$$f(v,u) + f(v+u,x) = f(u,x) + f(v,u+x),$$

so this multiplication is associative. Its identity is $(0, 0)$ and

$$(v, w)^{-1} = (v, w + f(v, v)).$$

Thus (2.2) defines a group G of order $2^{6+3} = 512$.

Identify W with the central subgroup $\{0\} \times W$. The square map is

$$q(v) = f(v,v) = (a + d + ae + bd,\ c + d + be + cd,\ b + c + ce). \tag{2.3}$$

Its polarization

$$\beta(v,u) = q(v+u) + q(v) + q(u) = f(v,u) + f(u,v) \tag{2.4}$$

is the commutator map. We use $[x, y] = x^{-1}y^{-1}xy$.

For clarity, the same group has generators $a, b, c, d, e, t, z_1, z_2, z_3$, where z_1, z_2, z_3 are the standard basis of W. The elements t, z_1, z_2, z_3 are central involutions, and

$$\begin{aligned} &a^2 = z_1, \quad b^2 = z_3, \quad c^2 = z_2 z_3, \quad d^2 = z_1 z_2, \quad e^2 = 1, \\ &[a,e] = [b,d] = z_1, \qquad [b,e] = [c,d] = z_2, \qquad [c,e] = z_3. \end{aligned} \tag{2.5}$$

All other pairs among a, b, c, d, e commute. These relations collect every word to

$$a^\alpha b^\beta c^\gamma d^\delta e^\varepsilon t^\tau z_1^{\eta_1} z_2^{\eta_2} z_3^{\eta_3}, \qquad \alpha, \ldots, \eta_3 \in \{0, 1\}.$$

The explicit model (2.2) has 512 elements and satisfies the relations, so all these normal forms are distinct.

The commutator values in (2.5) span W. Since all squares also lie in W, the identity $\Phi(G) = G^2 G'$ for a finite 2-group gives

$$G' = \Phi(G) = W. \tag{2.6}$$

The radical of β on V is $\langle t \rangle$. Hence

$$Z(G) = W \times \langle t \rangle \cong C_2^4.$$

The group is nonabelian because $[a, e] = z_1 \neq 1$. It has class two and exponent four. The coordinate t occurs in neither f nor q, so

$$G = H \times C_2, \qquad |H| = 256, \tag{2.7}$$

where H is obtained by omitting t from the presentation.

3 A direct count of endomorphisms

An endomorphism preserves $W = \Phi(G)$, and so induces linear maps $T : V \to V$ and $L : W \to W$ satisfying

$$q(Tv) = Lq(v) \qquad (v \in V). \tag{3.1}$$

Conversely, every pair satisfying (3.1) lifts to exactly 2^{18} endomorphisms: the W-components of the images of the six basis generators are arbitrary. Compatibility of all squares and commutators is precisely (3.1). We will show that

L	$\#\{T : qT = Lq\}$
0	$8\,128$
1_W	128
every other L	0.

(3.2)

3.1 The five-dimensional quadratic map

Write

$$V = V_0 \oplus \langle t \rangle, \qquad V_0 = \langle a, b, c, d, e \rangle,$$

and let $q_0 = q|_{V_0}$. The notation identifies basis vectors with their names in the presentation. From (2.3),

$$q_0^{-1}(0) = \{0, e, a + e\}. \tag{3.3}$$

For example, considering the four possible pairs (d, e) gives this list immediately. Directly from the commutators,

$$C_\beta(e) = \langle d, e \rangle, \qquad C_\beta(a + e) = \langle d, a + e \rangle \quad \text{inside } V_0, \tag{3.4}$$

where $C_\beta(x) = \{v : \beta(x, v) = 0\}$.

Lemma 3.1. *There is no three-dimensional $U \leq V_0$ with $\dim\langle q_0(U)\rangle \leq 1$, and no four-dimensional $U \leq V_0$ with $\dim\langle q_0(U)\rangle \leq 2$.*

Proof. For the first assertion, if the quadratic image is zero, then U has eight zero vectors, contradicting (3.3). Otherwise $q_0|_U$ is a scalar quadratic form times a fixed nonzero vector of W. Its alternating polarization in dimension three has a nonzero radical vector v. If $q_0(v) = 0$, then (3.3)–(3.4) force U into a two-dimensional β-centralizer. If $q_0(v) \neq 0$, translation by v interchanges the two values of $q_0|_U$, producing four zero vectors, again a contradiction.

For the second assertion, take a nonzero functional $\chi = (r, s, t)$ on W annihilating $q_0(U)$. The polar form of χq_0 pairs $\langle a, b, c \rangle$ with $\langle d, e \rangle$ through

$$M_\chi = \begin{pmatrix} 0 & r \\ r & s \\ s & t \end{pmatrix}. \tag{3.5}$$

If $(r, s) \neq (0, 0)$, this matrix has rank two. The full alternating form has rank four and radical dimension one, so a totally isotropic subspace has dimension at most three. If $\chi = (0, 0, 1)$, then $\chi q_0 = b + c + ce$, whose polar radical is $\langle a, b, d \rangle$. Any four-dimensional polar-isotropic subspace contains this radical, but $\chi q_0(b) = 1$. Thus it cannot be totally singular. □

3.2 Exclusion of ranks one and two for L

Given (3.1), let $M : V_0 \to V_0$ be $T|_{V_0}$ followed by projection along t. Then

$$q_0(Mv) = Lq_0(v). \tag{3.6}$$

Suppose first that L has rank one. Write Lq_0 as a nonzero scalar quadratic form times a nonzero vector of W. Its singular radical has dimension at most two. Indeed, (3.5) gives polar radical dimension one except for $\chi = (0, 0, 1)$; in that exception the singular radical is $\langle a, d\rangle$. Equation (3.6) puts $\ker M$ in this singular radical, so $\operatorname{rank} M \geq 3$. But $q_0(\operatorname{im} M)$ lies in a line, contradicting Lemma 3.1.

Suppose next that L has rank two, and put $J = \ker L$. For $v = (a, b, c, d, e)$, the polar values on the five basis vectors are

$$ez_1, \quad dz_1 + ez_2, \quad dz_2 + ez_3, \quad bz_1 + cz_2, \quad az_1 + bz_2 + cz_3. \tag{3.7}$$

For all five values to lie in the same line J, one must have $e = d = 0$, and then $c = b = 0$. Hence

$$\{v : \beta(v, V_0) \subseteq J\} \subseteq \langle a\rangle.$$

Polarizing (3.6) shows that $\ker M$ lies in this subspace. Thus $\operatorname{rank} M \geq 4$, while $q_0(\operatorname{im} M)$ lies in the plane $\operatorname{im} L$, again contradicting Lemma 3.1.

3.3 Invertible L

If L is invertible, (3.6) and its polarization imply that $\ker M$ is contained in the radical of the full W-valued form $\beta|_{V_0}$, which is zero. Thus M is invertible.

There are exactly two invertible compatible pairs (M, L). Both have $L = 1_W$; one has $M = 1_{V_0}$, and the other has

$$M(a) = a, \quad M(b) = b, \quad M(c) = c, \quad M(d) = d, \quad M(e) = e + a. \tag{3.8}$$

Here is a direct check of completeness. Equation (3.3) forces M to permute e and $a + e$, and hence to fix a. The map (3.8) preserves q_0; after composing with it if necessary, assume that M fixes both a and e. Then $Lz_1 = z_1$, and the pairing with a shows that M preserves the e-coordinate. Equation (3.4) now forces $M(d) = d$. Applying q_0 to d gives $Lz_2 = z_2$.

The pairings with d imply

$$M(b) = b + \alpha a + \gamma d, \qquad M(c) = c + \alpha' a + \gamma' d.$$

Pairing the first expression with e gives $\alpha = 0$; pairing the second gives $Lz_3 = z_3 + \alpha' z_1$. But

$$q_0(b + \gamma d) = z_3 + \gamma z_2,$$

so compatibility of the square of b forces $\gamma = \alpha' = 0$. Finally the square of c forces $\gamma' = 0$. Thus $M = L = 1$ after the initial composition, as claimed.

Since M is onto V_0, polar compatibility forces $T(t) \in \langle t\rangle$. For each of the two possibilities for M, the t-component of $T|_{V_0}$ is an arbitrary linear functional, with 2^5 choices, and $T(t)$ is either 0 or t. Hence there are

$$2 \cdot 2^5 \cdot 2 = 128$$

compatible maps T for $L = 1_W$. Exactly 64 are invertible.

3.4 The zero map L

For $L = 0$, the image of T must be totally singular. From (3.3), the complete zero set in V is

$$\{0, e, a+e, t, e+t, a+e+t\}.$$

It contains five singular lines and exactly two singular planes, $\langle e, t\rangle$ and $\langle a+e, t\rangle$, and no larger singular subspace. Counting T by its exact image gives

$$1 + 5(2^6 - 1) + 2(2^6 - 1)(2^6 - 2) = 8\,128.$$

This proves (3.2). Consequently,

$$E(G) = (8\,128 + 128)2^{18} = 129 \cdot 2^{24}. \tag{3.9}$$

Likewise,

$$|\operatorname{Aut}(G)| = 64 \cdot 2^{18} = 2^{24}. \tag{3.10}$$

Together with (4.10), established in Section 4, this proves Theorem 1.1.

4 Counting subgroups and partial isomorphisms

4.1 The two weighted counting identities

For an isomorphism type X, let s_X be the number of subgroups of G isomorphic to X, and let q_X be the number of normal subgroups $N \triangleleft G$ with $G/N \cong X$. Put $a_X = |\operatorname{Aut}(X)|$. Then

$$P(G) := |\operatorname{PIso}(G)| = \sum_X a_X s_X^2, \qquad E(G) := |\operatorname{End}(G)| = \sum_X a_X s_X q_X. \tag{4.1}$$

For the first identity, choose an ordered pair of subgroups of type X and an isomorphism between them. For the second, choose a kernel, an image subgroup, and an isomorphism from the quotient to the image. There are a_X isomorphisms in either case.

4.2 Enumeration by binary subspaces

Let $\pi : G \to V = G/W$ be the quotient map.

Proposition 4.1. *Fix subspaces $U \le V$ and $S \le W$. Subgroups $K \le G$ with $\pi(K) = U$ and $K \cap W = S$ exist if and only if*

$$q(U) \subseteq S. \tag{4.2}$$

When they exist, their number is

$$m(U, S) = 2^{\dim U(3 - \dim S)}. \tag{4.3}$$

All have the same isomorphism type, represented by $q|_U : U \to S$. They are normal in G if and only if

$$\beta(U, V) \subseteq S. \tag{4.4}$$

In that case all corresponding quotients have the quadratic-map type

$$\bar{q} : V/U \longrightarrow W/S, \qquad v + U \longmapsto q(v) + S. \tag{4.5}$$

Proof. A subgroup K with the stated properties has $K/S \cong U$ elementary abelian, so its squares force (4.2). Conversely, that condition makes $\pi^{-1}(U)/S$ elementary abelian: all its squares are trivial, and polarization also kills all its commutators. The possible K/S are precisely the complements to W/S in this vector space. They form an affine space over $\mathrm{Hom}(U, W/S)$, proving (4.3).

The squares and commutators of lifts of a basis of U are independent of the chosen complement, since W is central of exponent two. They are prescribed by $q|_U$ and its polarization. Thus the isomorphism type is independent of the complement. Finally, K is normal exactly when $[K, G] \le K \cap W = S$, which is (4.4). Under both conditions, (4.5) is well defined and prescribes the squares and commutators of a generating set of G/K. □

Every subgroup gives one and only one pair (U, S). Thus enumerating all subspaces of $\mathbf{F}_2^6$ and $\mathbf{F}_2^3$ and applying Proposition 4.1 is exhaustive, with exact multiplicities and without enumeration up to conjugacy.

4.3 Exact isomorphism tests and automorphism orders

The groups encountered in Proposition 4.1 have central elementary abelian Frattini subgroup. The following reduction both identifies their types and computes the weights in (4.1).

For a quadratic map $q_D : D \to Z$ over $\mathbf{F}_2$, replace Z by

$$F = \langle q_D(D) \rangle.$$

This is the Frattini subgroup of the represented group. A complement to F in Z splits off as a central elementary abelian direct factor. Next let

$$R_0 = \{v \in D : q_D(v) = 0,\ \beta_D(v, x) = 0 \text{ for all } x \in D\}$$

be the singular radical. This is a subspace, and q_D is constant on its cosets. The corresponding central involutions also split off. The reduced quadratic map is the induced map on D/R_0 with values in F.

The resulting group has the form

$$C \times C_2^r, \tag{4.6}$$

where C has no direct factor C_2 and $\Omega_1(Z(C)) = \Phi(C)$. Both the reduced quadratic-map type and r are intrinsic: the removed radical is canonical, and any complement gives the same induced map on the quotient.

Lemma 4.2. *Let C_1, C_2 be two such reduced groups, with square maps $q_i : D_i \to F_i$. They are isomorphic if and only if there are invertible linear maps $T : D_1 \to D_2$ and $L : F_1 \to F_2$ such that*

$$q_2(Tv) = Lq_1(v) \qquad (v \in D_1). \tag{4.7}$$

If $d = \dim D_1 = \dim D_2$ and $z = \dim F_1 = \dim F_2$, then each such pair has exactly 2^{dz} isomorphism lifts. In particular,

$$|\operatorname{Aut}(C)| = 2^{dz} \#\{(T, L) \in \mathrm{GL}_d(2) \times \mathrm{GL}_z(2) : q_C T = L q_C\}. \tag{4.8}$$

Furthermore,

$$|\operatorname{Aut}(C \times C_2^r)| = |\operatorname{Aut}(C)|\, 2^{r(d+z)} |\mathrm{GL}_r(2)|, \tag{4.9}$$

where $|\mathrm{GL}_0(2)| = 1$.

Proof. The Frattini subgroup is characteristic. An isomorphism therefore induces T and L, necessarily satisfying (4.7). Conversely, squares of basis lifts and their pairwise commutators give a presentation of the group. Equation (4.7), together with its polarization, preserves all these relations. Each of the d basis images can independently be multiplied by any element of the target Frattini subgroup F_2, which gives 2^{dz} lifts. They are surjective, and hence isomorphisms.

For (4.9), write an automorphism in blocks relative to $C \times C_2^r$. In addition to automorphisms of C and C_2^r, its off-diagonal blocks are arbitrary homomorphisms $C \to C_2^r$ and $C_2^r \to \Omega_1(Z(C)) = \Phi(C)$, giving 2^{rd} and 2^{rz} choices. The latter block is invisible on the Frattini quotient, so the diagonal blocks must be invertible. Conversely, invertible diagonal blocks and arbitrary off-diagonal blocks induce an invertible map on the Frattini quotient and thus an automorphism. □

The verifier enumerates all possible L and all ordered images of a basis under T, enforcing linear independence when required. It checks the square values and all pairwise polar values. These checks are equivalent to (4.7) on the entire vector space. Every candidate is compared with every previously found reduced core of the same pair of dimensions. No group database or heuristic isomorphism test is used.

4.4 The resulting count

The enumeration gives Table 1. The column $\sum q_X$ counts kernels giving a quotient of the displayed order; it is not the number of normal subgroups of that order. The unweighted

Table 1: Exact counts grouped by the order of the isomorphism type.

$\lvert X\rvert$	$\sum s_X$	$\sum q_X$	$\sum a_X s_X^2$	$\sum a_X s_X q_X$
1	1	1	1	1
2	47	63	2 209	2 961
4	507	651	561 398	1 074 150
8	1 363	1 395	21 820 072	69 136 200
16	2 563	659	196 562 880	800 573 760
32	2 531	111	657 056 768	1 259 919 360
64	1 635	63	749 027 328	0
128	651	43	386 138 112	0
256	63	15	136 314 880	16 777 216
512	1	1	16 777 216	16 777 216
Total	9 362	3 002	2 164 260 864	2 164 260 864

aggregate columns alone are not sufficient to reconstruct the weighted sums. Appendix A gives all 151 type records, with representatives and automorphism orders, from which the weighted columns are obtained directly by (4.1). There are 123 subgroup types and 36 quotient types, using 63 reduced quadratic-map cores.

In particular, the exhaustive count proves

$$P(G) = 2\,164\,260\,864. \tag{4.10}$$

The second weighted sum gives the same value for $E(G)$. The direct derivation in Section 3 does not use the subgroup-type classification.

5 Reproducibility and scope

5.1 The two verification programs

The source file `verify_counterexample.py` uses only the Python standard library (Python 3.10 or later). It starts from the square and commutator values in (2.5), enumerates all binary subspaces, applies Proposition 4.1, and performs the exhaustive isomorphism tests of Lemma 4.2. It then writes `counterexample_certificate.json` and `counts_by_order.csv`. These files are outputs, never inputs.

The command is

```
python verify_counterexample.py
```

The same program separately considers all $2^9 = 512$ linear maps $L : W \to W$ and counts every compatible T by exact backtracking, without using subgroup types. Its key output is

```
P = 2164260864  E = 2164260864  D = 0
Compatible pairs:  8256  lifts per pair:  262144
E_direct:  2164260864
Compatible invertible pairs:  64  Aut(G): 16777216
ALL CHECKS PASSED
```

The separate C++17 program `verify_cayley.cpp` constructs the actual 512×512 multiplication table from (2.1), checks the identity, inverses, and all 512^3 associativity identities, and enumerates subgroups by index-two extensions using group multiplication. Every nontrivial subgroup is a finite 2-group and has an index-two subgroup, so this enumeration is exhaustive. Duplicate subgroups are removed by comparing their element sets. Normality is checked using commutators with the generators. Run

```
g++ -O2 -std=c++17 verify_cayley.cpp -o verify_cayley
./verify_cayley
```

It finds 9 362 subgroups, 3 002 normal subgroups, and a center of order 16, with the order distributions in Table 1 (the normal-subgroup distribution reverses the quotient-order column). This is an independent check of the group law and unweighted subgroup counts; it is *not* a second quadratic-map classification. The weighted calculation of $P(G)$ is performed by the Python verifier. Neither program uses GAP, SageMath, a SmallGroups database, or stored isomorphism data.

The supplied run logs record successful executions of both programs. The weighted counts were reproduced, and the regenerated JSON certificate agreed byte-for-byte with the earlier certificate. The PDF includes the two program sources, the JSON certificate, the CSV table, and the recorded run logs as embedded file attachments. Extract them into one directory to run the commands above. The embedded `SHA256SUMS` manifest records cryptographic hashes of the accompanying files. The printed certificate is complete; the machine-readable version is supplied for convenient checking.

5.2 Scope of the conclusion

The construction was found by varying square maps with fixed commutator data in groups of order 256 and testing a central C_2-factor. The final count was regenerated from the explicit multiplication law; it does not depend on the discovery database or on earlier proposed structural lemmas. No claim that order 512 is minimal is made.

Corollary 5.1. *If A is any finite abelian group of odd order, then $G \times A$ is a nonabelian group with $|\mathrm{PIso}(G \times A)| = |\mathrm{End}(G \times A)|$.*

Proof. For finite groups of coprime orders, every subgroup of their direct product is a product of subgroups, and every homomorphism respects the two primary components. Thus

$$P(G \times A) = P(G)P(A), \qquad E(G \times A) = E(G)E(A).$$

Apply Theorem 1.1 and Cameron's equality for A. □

Acknowledgement

This work was carried out with assistance from ChatGPT.

References

[1] P. J. Cameron, *Endomorphisms and partial isomorphisms*, Semigroup Forum **111** (2025), 538–539. doi:10.1007/s00233-025-10514-5.

[2] E. I. Khukhro and V. D. Mazurov (eds.), *Unsolved Problems in Group Theory. The Kourovka Notebook*, 21st ed., Novosibirsk, 2026, version 46, Problem 19.20, p. 135. arXiv:1401.0300v46.

A Complete printable counting certificate

The tables below encode all 151 isomorphism types occurring as subgroups or quotients of G. The indices are internal labels of the verifier, not SmallGroups identifiers.

A.1 Reduced quadratic-map representatives

For each core K_i, let

$$d_i = \dim K_i/\Phi(K_i), \qquad z_i = \dim \Phi(K_i), \qquad b_i = |\operatorname{Aut}(K_i)|.$$

The row specifies the square values $\sigma_j = q_i(e_j)$ and the polar values $\gamma_{jk} = \beta_i(e_j, e_k)$, with pairs (j,k) in lexicographic order. A number n between 0 and $2^{z_i} - 1$ encodes the vector

$$n = \sum_{h=1}^{z_i} \epsilon_h 2^{h-1} \quad \longleftrightarrow \quad \sum_{h=1}^{z_i} \epsilon_h z_h.$$

Thus addition of encoded vectors is bitwise exclusive-or, not integer addition. The complete map is recovered from

$$q_i\left(\sum_j x_j e_j\right) = \sum_j x_j \sigma_j + \sum_{j<k} x_j x_k \gamma_{jk}. \tag{A.1}$$

The tuple γ is empty when $d_i \le 1$. Core K_0 is the trivial group. The counterexample is the type $(i,r) = (1,1)$, namely $K_1 \times C_2$.

Table 2: The reduced cores K_i.

i	d_i, z_i	b_i	σ	γ
0	0,0	1	∅	∅
1	5,3	65 536	(1,2,4,7,0)	(0,0,0,1,0,1,6,6,2,0)
2	4,2	1 024	(1,2,3,0)	(0,0,3,3,1,0)
3	5,2	4 096	(1,2,3,0,0)	(0,0,0,1,0,1,1,1,2,0)
4	5,2	4 096	(1,1,2,2,0)	(0,0,0,1,0,1,3,3,1,0)
5	5,2	4 096	(1,2,1,2,0)	(0,0,0,1,0,1,3,3,2,0)
6	5,2	8 192	(1,2,2,1,0)	(0,0,0,1,0,1,0,0,2,0)
7	5,2	4 096	(1,2,0,3,0)	(0,0,0,1,0,1,2,2,2,0)
8	5,2	16 384	(1,0,2,3,0)	(0,0,0,1,0,1,2,2,0,0)
9	3,1	48	(1,1,0)	(0,0,1)
10	4,1	1 920	(1,1,1,0)	(0,0,1,1,0,0)
11	5,1	23 040	(1,1,0,0,0)	(0,0,0,1,0,1,1,1,1,0)
12	4,1	1 152	(1,0,0,0)	(0,0,1,1,1,0)
13	1,1	2	(1)	∅
14	2,2	96	(1,2)	(0)
15	2,3	384	(1,2)	(7)
16	2,2	32	(0,1)	(3)
17	2,2	32	(1,2)	(1)
18	2,1	24	(1,1)	(1)
19	2,1	8	(1,0)	(1)
20	3,3	86 016	(1,2,4)	(0,0,0)
21	3,3	512	(1,2,3)	(7,1,0)
22	3,2	192	(0,1,2)	(3,1,0)
23	3,3	1 024	(1,2,4)	(1,4,0)
24	3,3	2 048	(1,2,2)	(0,0,4)

Continued on the next page.

Table 2 continued: reduced cores.

i	d_i, z_i	b_i	σ	γ
25	3,3	1 024	(1,2,2)	(1,2,4)
26	3,2	256	(1,2,2)	(0,1,3)
27	3,3	512	(0,1,1)	(3,5,5)
28	3,3	12 288	(1,2,4)	(1,0,4)
29	3,3	1 024	(0,1,4)	(3,1,4)
30	3,3	12 288	(1,2,4)	(0,0,1)
31	3,3	1 024	(1,2,4)	(7,2,3)
32	3,3	1 536	(0,1,4)	(3,6,1)
33	3,3	4 096	(1,2,1)	(7,3,4)
34	3,3	2 048	(1,2,3)	(0,6,5)
35	3,3	2 048	(0,1,4)	(3,0,7)
36	3,2	384	(1,2,3)	(0,0,3)
37	3,3	4 096	(0,1,3)	(3,0,6)
38	3,3	3 072	(1,2,4)	(7,1,5)
39	3,2	128	(0,1,2)	(3,0,2)
40	3,3	2 048	(1,2,0)	(0,1,6)
41	3,3	1 024	(0,1,4)	(3,0,2)
42	3,2	128	(1,2,0)	(0,1,0)
43	4,3	16 384	(1,2,4,7)	(0,0,0,0,1,6)
44	4,3	8 192	(0,1,2,4)	(3,1,0,0,7,3)
45	4,3	16 384	(1,2,2,7)	(1,0,0,4,1,6)
46	4,3	4 096	(0,1,1,3)	(3,5,0,5,7,4)
47	4,3	16 384	(1,2,4,5)	(0,1,0,4,1,4)
48	4,3	4 096	(0,1,3,5)	(3,7,0,3,6,3)
49	4,3	16 384	(1,2,4,5)	(1,1,0,2,1,4)
50	4,3	4 096	(0,1,4,3)	(3,2,0,1,7,4)
51	4,3	65 536	(1,2,4,7)	(0,0,1,0,7,4)
52	4,3	4 096	(0,1,2,4)	(3,1,7,0,4,2)
53	4,3	8 192	(1,2,2,7)	(1,0,1,4,7,2)
54	4,3	16 384	(1,2,4,5)	(0,1,1,4,5,6)
55	4,3	8 192	(1,2,4,5)	(1,1,1,2,5,2)
56	4,3	4 096	(0,1,4,3)	(3,2,7,1,3,1)
57	4,3	24 576	(1,2,4,0)	(0,0,1,0,6,2)
58	4,3	8 192	(1,2,2,0)	(0,0,1,4,4,6)
59	4,3	24 576	(1,2,4,0)	(0,0,1,1,7,2)
60	4,3	16 384	(1,2,4,0)	(0,0,1,1,5,0)
61	4,3	16 384	(1,2,3,0)	(0,0,1,3,6,0)
62	4,3	16 384	(1,2,4,0)	(0,0,1,5,7,0)

A.2 All subgroup and quotient types

Each row of Table 3 represents

$$X = K_i \times C_2^r, \qquad |X| = 2^{d_i+z_i+r}.$$

The symbols s_X, q_X have the meanings in Section 4, and

$$a_X = b_i\, 2^{r(d_i+z_i)} \prod_{j=0}^{r-1} (2^r - 2^j).$$

All rows, including those with $s_X = 0$, are displayed. The full sums are

$$\sum s_X = 9\,362, \quad \sum q_X = 3\,002, \quad \sum a_X s_X^2 = \sum a_X s_X q_X = 2\,164\,260\,864.$$

The machine-readable JSON file additionally records both weighted contributions row by row. They are obtained directly by multiplying the printed integers; no further mathematical classification is needed.

Table 3: Complete type-by-type subgroup and quotient certificate.

i	r	$\lvert X\rvert$	a_X	s_X	q_X
0	0	1	1	1	1
0	1	2	1	47	63
0	2	4	6	275	651
0	3	8	168	295	1 395
0	4	16	20 160	61	651
0	5	32	9 999 360	2	63
0	6	64	20 158 709 760	0	1
1	0	256	65 536	32	8
1	1	512	16 777 216	1	1
2	0	64	1 024	0	16
2	1	128	65 536	0	12
2	2	256	25 165 824	0	1
3	0	128	4 096	0	4
3	1	256	524 288	0	1
4	0	128	4 096	0	4
4	1	256	524 288	0	1
5	0	128	4 096	0	4
5	1	256	524 288	0	1
6	0	128	8 192	0	4
6	1	256	1 048 576	0	1
7	0	128	4 096	0	4
7	1	256	524 288	0	1
8	0	128	16 384	0	4
8	1	256	2 097 152	0	1
9	0	16	48	0	8
9	1	32	768	0	28
9	2	64	73 728	0	14
9	3	128	33 030 144	0	1
10	0	32	1 920	0	12
10	1	64	61 440	0	18
10	2	128	11 796 480	0	3
11	0	64	23 040	0	2
11	1	128	1 474 560	0	1
12	0	32	1 152	0	8
12	1	64	36 864	0	12
12	2	128	7 077 888	0	2
13	0	4	2	232	0
13	1	8	8	940	0
13	2	16	192	630	0
13	3	32	21 504	85	0
13	4	64	10 321 920	2	0
14	0	16	96	272	0
14	1	32	1 536	204	0
14	2	64	147 456	17	0
15	0	32	384	192	0
15	1	64	12 288	48	0
16	0	16	32	416	0
16	1	32	512	312	0
16	2	64	49 152	26	0
17	0	16	32	960	0
17	1	32	512	720	0
17	2	64	49 152	60	0
18	0	8	24	64	0

Continued on the next page.

Table 3 continued: full type certificate.

i	r	$\lvert X\rvert$	a_X	s_X	q_X
18	1	16	192	112	0
18	2	32	9 216	28	0
18	3	64	2 064 384	1	0
19	0	8	8	64	0
19	1	16	64	112	0
19	2	32	3 072	28	0
19	3	64	688 128	1	0
20	0	64	86 016	8	0
20	1	128	5 505 024	1	0
21	0	64	512	96	0
21	1	128	32 768	12	0
22	0	32	192	384	0
22	1	64	6 144	144	0
22	2	128	1 179 648	6	0
23	0	64	1 024	256	0
23	1	128	65 536	32	0
24	0	64	2 048	48	0
24	1	128	131 072	6	0
25	0	64	1 024	112	0
25	1	128	65 536	14	0
26	0	32	256	320	0
26	1	64	8 192	120	0
26	2	128	1 572 864	5	0
27	0	64	512	112	0
27	1	128	32 768	14	0
28	0	64	12 288	32	0
28	1	128	786 432	4	0
29	0	64	1 024	80	0
29	1	128	65 536	10	0
30	0	64	12 288	16	0
30	1	128	786 432	2	0
31	0	64	1 024	64	0
31	1	128	65 536	8	0
32	0	64	1 536	112	0
32	1	128	98 304	14	0
33	0	64	4 096	24	0
33	1	128	262 144	3	0
34	0	64	2 048	16	0
34	1	128	131 072	2	0
35	0	64	2 048	32	0
35	1	128	131 072	4	0
36	0	32	384	64	0
36	1	64	12 288	24	0
36	2	128	2 359 296	1	0
37	0	64	4 096	16	0
37	1	128	262 144	2	0
38	0	64	3 072	16	0
38	1	128	196 608	2	0
39	0	32	128	128	0
39	1	64	4 096	48	0
39	2	128	786 432	2	0
40	0	64	2 048	48	0
40	1	128	131 072	6	0
41	0	64	1 024	32	0
41	1	128	65 536	4	0
42	0	32	128	64	0
42	1	64	4 096	24	0
42	2	128	786 432	1	0
43	0	128	16 384	16	0

Continued on the next page.

Table 3 continued: full type certificate.

i	r	$\lvert X\rvert$	a_X	s_X	q_X
43	1	256	2 097 152	1	0
44	0	128	8 192	32	0
44	1	256	1 048 576	2	0
45	0	128	16 384	16	0
45	1	256	2 097 152	1	0
46	0	128	4 096	32	0
46	1	256	524 288	2	0
47	0	128	16 384	16	0
47	1	256	2 097 152	1	0
48	0	128	4 096	32	0
48	1	256	524 288	2	0
49	0	128	16 384	16	0
49	1	256	2 097 152	1	0
50	0	128	4 096	32	0
50	1	256	524 288	2	0
51	0	128	65 536	16	0
51	1	256	8 388 608	1	0
52	0	128	4 096	96	0
52	1	256	524 288	6	0
53	0	128	8 192	16	0
53	1	256	1 048 576	1	0
54	0	128	16 384	16	0
54	1	256	2 097 152	1	0
55	0	128	8 192	16	0
55	1	256	1 048 576	1	0
56	0	128	4 096	32	0
56	1	256	524 288	2	0
57	0	128	24 576	16	0
57	1	256	3 145 728	1	0
58	0	128	8 192	32	0
58	1	256	1 048 576	2	0
59	0	128	24 576	16	0
59	1	256	3 145 728	1	0
60	0	128	16 384	16	0
60	1	256	2 097 152	1	0
61	0	128	16 384	16	0
61	1	256	2 097 152	1	0
62	0	128	16 384	16	0
62	1	256	2 097 152	1	0

The PDF also contains the verification programs, their recorded run logs, the machine-readable tables, and a `SHA256SUMS` manifest as embedded attachments. The hashes identify exact files; the mathematical content is the proof and complete certificate above.